

CLAIMS

What is claimed is:

1. A method, comprising:
loading authenticated/trusted power management code into a memory of a secure environment of an operating system (OS); and
executing the power management code within the secure environment of the OS to handle power management tasks.
2. The method of claim 1, further comprising determining whether the secure environment of the OS has been activated, the loading and executing the power management code being performed if the secure environment is activated.
3. The method of claim 2, wherein the secure environment of the OS is launched and executed within a virtual machine (VM) within the OS, and wherein the OS includes a plurality of VMs having a task carried out by the respective VM.
4. The method of claim 3, further comprising monitoring activities of the respective VM including whether the secure environment is about to terminate.
5. The method of claim 1, further comprising:
determining whether the secure environment of the OS is about to terminate; and
terminating and unloading the power management code from the memory prior to terminating the secure environment of the OS.

6. The method of claim 1, wherein the secure environment is launched in response to an initiation of a secure transaction by a user.
7. The method of claim 1, further comprising authenticating the power management code to determine whether the power management code is trusted.
8. The method of claim 7, wherein authenticating the power management code comprises:
 - retrieving a public key from the power management code;
 - computing, via one or more hash operations, a hash of the public key; and
 - comparing, the computed hash of the public key with a public key hash stored outside of the power management code to authenticate the power management code.
9. The method of claim 8, further comprising verifying images of one or more modules within the power management code.
10. The method of claim 9, wherein verifying the images comprises:
 - decrypting a signature block of the power management code to form a first module hash block;
 - performing one or more hash operations on at least one portions of the power management code to generate a second module hash block; and
 - comparing the first and second module hash blocks to verify the one or more modules.
11. A machine-readable medium having executable code to cause a machine to perform a method for power management, the method comprising:

loading authenticated/trusted power management code into a memory of a secure environment of an operating system (OS); and
executing the power management code within the secure environment of the OS to handle power management tasks.

12. The machine-readable medium of claim 11, wherein the method further comprises determining whether the secure environment of the OS has been activated, the loading and executing the power management code being performed if the secure environment is activated.
13. The machine-readable medium of claim 12, wherein the secure environment of the OS is launched and executed within a virtual machine (VM) within the OS, and wherein the OS includes a plurality of VMs having a task carried out by the respective VM.
14. The machine-readable medium of claim 13, wherein the method further comprises monitoring activities of the respective VM including whether the secure environment is about to terminate.
15. The machine-readable medium of claim 11, wherein the method further comprises:
determining whether the secure environment of the OS is about to terminate; and
terminating and unloading the power management code from the memory prior to terminating the secure environment of the OS.
16. The machine-readable medium of claim 11, wherein the secure environment is launched in response to an initiation of a secure transaction by a user.

17. The machine-readable medium of claim 11, further comprising authenticating the power management code to determine whether the power management code is trusted.
18. The machine-readable medium of claim 17, wherein authenticating the power management code comprises:
 - retrieving a public key from the power management code;
 - computing, via one or more hash operations, a hash of the public key; and
 - comparing the computed hash of the public key with a public key hash stored outside of the power management code to authenticate the power management code.
19. The machine-readable medium of claim 18, wherein the method further comprises verifying images of one or more modules within the power management code.
20. The machine-readable medium of claim 19, wherein verifying the images comprises:
 - decrypting a signature block of the power management code to form a first module hash block;
 - performing one or more hash operations on at least one portions of the power management code to generate a second module hash block; and
 - comparing the first and second module hash blocks to verify the one or more modules.
21. A data processing system, comprising:
 - a processor capable of executing one or more processes in one or more secure environment respectively;
 - a memory coupled to the processor; and

a process executed by the processor from the memory to cause the processor to
load authenticated/trusted power management code into a memory of a secure
environment of an operating system (OS) and
execute the power management code within the secure environment of the OS
to handle power management tasks.

22. The data processing system of claim 21, wherein the process further causes the processor to:

determine whether the secure environment of the OS is about to terminate; and
terminate and unload the power management code from the memory prior to
terminating the secure environment of the OS.

23. A method, comprising:

launching a secure computing environment within an operating system of a data
processing system in response to a request from a transaction;
dynamically loading a power management code for handling power management
during launching the secure computing environment; and
dynamically unloading the power management code when the secure computing
environment is terminated.

24. The method of claim 23, further comprising authenticating the power management code
prior to loading the power management code.

25. The method of claim 24, wherein authenticating the power management code comprises
verifying a first key stored within the power management code against with a second key

stored outside of the power management code, and wherein the first key is stored in the power management code during manufacturing of the power management code.

26. The method of claim 25, wherein authenticating the power management code further comprises performing a checksum operation on at least a portion of the power management code.
27. The method of claim 23, wherein the secure environment and the power management code are loaded in a dedicated memory protected by at least one of software and hardware, and wherein the dedicated memory is not accessible by other non-secure components of the data processing system.
28. A machine-readable medium having executable code to cause a machine to perform a method for power management, the method comprising:
 - launching a secure computing environment within an operating system of a data processing system in response to a request from a transaction;
 - dynamically loading a power management code for handling power management during launching the secure computing environment; and
 - dynamically unloading the power management code when the secure computing environment is terminated.
29. The machine-readable medium of claim 28, wherein the method further comprises authenticating the power management code prior to loading the power management code.

30. The machine-readable medium of claim 29, wherein authenticating the power management code comprises verifying a first key stored within the power management code against with a second key stored outside of the power management code, and wherein the first key is stored in the power management code during manufacturing of the power management code.